10/508840
JT12 Rec'd PCT/PTO 21 SEP 2004

Express Mail Mailing Label
No. ER 936794134 US

14/Pats

Selective Multimedia Data Encryption

The present invention relates to a conditional access system wherein digitised multimedia data are transmitted in a continuous transport stream of successive data packets. The invention also relates to a method of producing a partially scrambled or corrupted transport stream from a clear transport stream containing digitised multimedia data in successive data packets.

Data security is an important aspect in multimedia commerce. Conditional access systems (CAS) mainly rely on scrambling of a transport stream containing protected multimedia contents. In Digital Video Broadcast ("DVB"), for example, only subscribers with a conditional access module ("CAM") and a valid subscriber card (Smart Card "SC") can descramble a scrambled transport stream and obtain TV contents in the clear for application to a TV set. The conditional access module must have the capability to process an MPEG stream in real-time at a processing rate of at least about 1.5 MB/sec, thereby placing high demands of performance on the hardware used in the CAM.

The present invention provides a conditional access system for multimedia data that offers acceptable security at drastically reduced requirements on hardware performance. For specific embodiments that include decryption circuitry inside a user smart card, the level of security of such system is even higher than that of conventional ones.

According to the invention, a selectively encrypted transport stream is formed from a base transport stream by detecting particular data packets within the base transport stream, removing and encrypting the particular data packets with an event encryption key, and inserting the encrypted data packets into the remaining base transport stream at insertion positions corresponding to the original positions

of the particular data packets in the base transport stream. Since only selected data packets must be processed for encryption/decryption, the amount of processing is drastically reduced.

According to a specific embodiment of the invention, a selectively encrypted transport stream is formed from a base transport stream by detecting particular data packets within the base transport stream, removing and encrypting the particular data packets with an event's encryption key, and inserting the encrypted data packets into the remaining base transport stream at insertion positions ahead in time with respect to the original positions of the particular data packets in the base transport stream.

In one aspect of the invention, the base transport stream is a clear transport stream, i.e. data are not scrambled. By selectively encrypting the transport stream, a high level of security is achieved even if the base transport stream is in the clear, because only selected data packets must be decrypted and decryption can be done with low-performance hardware such as can be embodied in a smart-card (Smart Card) - which is inherently safe.

In another aspect of the invention, the base transport stream is a scrambled transport stream, i.e. data are scrambled in accordance with a specific standard, such as the DVB standard. By selectively encrypting the scrambled transport stream, a high level of security is added to that achieved by scrambling.

The invention uses the fact that in a typical compressed multimedia data stream such as an MPEG stream, the contents of particular data packets are propagated to successive data packets, i.e. successive data packets are dependant on contents of preceding data packets, so that by encrypting only particular data packets, many successive data packets are affected, resulting in a sufficient overall scrambling of the data stream. Given the moderate hardware requirements, decryption can be performed by available Smart Cards, enabling a hardware implementation where the security entirely resides in the Smart Card.

Further, because the key can be changed frequently and a highly efficient encryption algorithm such as, for example, DES or 3DES can be used, the security in the proposed system is sufficient for the particular needs. A possibility to enhance security is to use a non public encryption algorithm.

For low value multimedia contents, or in a pay-per-event environment, it will generally be sufficient to send a fixed event decryption key prior to actual transmission of the selectively encrypted transport stream. For higher value multimedia contents, the event decryption key can be changed frequently. In a DVB environment, for example, the event decryption keys can be transmitted with the EMMs (Entitlement Management Message) in the transport stream. A user key available in the user smart card (Subscriber Card) will be used to decrypt in the EMMs, the event decryption keys. Another possibility is to have the event decryption key available in an one-event smart card, that will be sold to users.

In the preferred embodiment of the invention, the event decryption key is transmitted to an authorised receiver provided with a "light" conditional access module. As used here, "light" means that the conditional access module will not necessarily include hardware or software decryption or descrambling resources as the decryption may be performed in the user smart card. The selectively encrypted transport stream is transmitted to the receiver. The light conditional access module detects encrypted data packets, removes the encrypted data packets from the received transport stream, decrypts the encrypted data packets with the event decryption key, and inserts the decrypted data packets into the remaining received transport stream at positions corresponding to the respective original positions of the particular data packets within the clear transport stream. Preferably, the encrypted data packets are inserted at positions a predetermined number of data packets ahead of respective original positions.

Further advantages and features of the invention will appear from the following description of preferred embodiments with reference to the drawings. In the drawings:

Figs. 1 to 6 are block diagrams with descriptive legends for different embodiments of a head-end equipment for producing selectively encrypted data streams containing digitised multimedia data;

Figs. 7 to 10 are block diagrams with descriptive legends for different embodiments of a user equipment for decoding selectively encrypted data streams containing digitised multimedia data;

Fig. 11 is a diagram illustrating a first embodiment of a method of producing a scrambled or corrupted transport stream from a clear transport stream by selective encryption;

Fig. 12 is a diagram illustrating a method of producing a clear transport stream from a scrambled or corrupted transport stream produced with the method of Fig. 11;

Fig. 13 is a diagram illustrating a second embodiment of a method of producing a scrambled or corrupted transport stream from a clear transport stream by selective encryption; and

Fig. 14 is a diagram illustrating a third embodiment of a method of producing a scrambled or corrupted transport stream from a clear transport stream by selective encryption, wherein the scrambled or corrupted transport stream consists of selectively encrypted packets and DVB scrambled packets.

With reference now to Fig. 1, a first embodiment of a head-end component is shown for producing a selectively encrypted transport stream containing digital multimedia data. Specifically, the component includes a head-end PC (Personal Computer) 10 with an interface 12 for an SC (Smart Card) 14 and a serial high speed bi-directional communication interface 16 (e.g. a 1394 or a USB2 interface). The SC 14 has an internal processor with scrambling or encrypting capability and a safe memory for storing a plurality of private user keys. The head-end component further includes a professional (transmitter) STB (Set-Top-Box) 18 that has CI (Common Interface) and TS (Transport Stream) interface 20

and an RF port 22 for connection to a satellite link 24. The head-end component finally includes an interface module 26 to establish a high-speed serial connection between interface 20 of STB 18 and interface 16 of PC 10. Module 26 is preferably a PC card according to the PCMCIA standard and includes a microprocessor and a memory in addition to a CI and TS interface and a high-speed serial interface.

With reference to Fig. 11, to generate a selectively encrypted transport stream SETS from a base transport stream BTS consisting of successive digital data packets numbered 1, 2, ... 13 ..., selected data packets are extracted from the BTS and encrypted, or scrambled, with circuitry on SC 14, using an "event key". In the Fig. 1 embodiment, the BTS is a clear digital transport stream consisting of successive data packets and available within the PC 10. In Fig. 11, the encryption or scrambling step is referred to as "Packet scrambling". It should be understood that the base transport stream BTS can be a clear TS as indicated in Fig. 11, or a scrambled transport stream and, in particular, a conventional DVB-scrambled transport stream.

The keys used in the selective encryption/scrambling method include a user key pair and an event key pair, as indicated in Fig. 1, and each key pair can be symmetric or asymmetric, as also indicated in Fig. 1. The user keys (user_key_2) are stored in the memory of SC 14 in the case of private keys (public and private key pairs). The user keys are transmitted with the EMM in a DVB environment for decryption of the event keys used for the selective encryption/scrambling.

In the next step, referred to as "Packet buffering/insertion" in Fig. 11, the encrypted or scrambled data packets are inserted into the buffered transport stream at positions in time ahead of corresponding positions in the original BTS. For example, scrambled data packet #2 is inserted between data packet # -3 and data packet # -1, and now available position between data packets #1 and #3 is filled with scrambled data packet #5. As a result, a selectively encrypted, or scrambled, transport stream SETS is provided, as shown in Fig. 11.

The SETS is communicated to the STB 18 via module 26 for broadcast transmission over satellite link 24, as seen in Fig. 1.

With reference to Fig. 7, a first embodiment of a user-end component is shown for recovering in accordance with the method illustrated in Fig. 12, from a selectively encrypted transport stream, as may be produced with the component in Fig. 1 and in accordance with the Fig. 11 method, a clear transport stream.

The user component shown in Fig. 7 includes a PC card module 30 referred to as a "Selective Crypto Module", that includes a CI & TS interface 32 (Common Interface and interface for Transport Stream), an incorporated smart-card reader 34, a microprocessor with memory unit 36 and a packet filtering and insertion logic 38. The user component works with a smart-card 40 to be inserted in the reader 34 and referred to in Fig. 7 as a "Pay Per Event Smart Card". Of course, this is just one of many possible scenarios in a protected DVB environment.

The module 30 is inserted into a CI slot of a conventional Set-Top-Box that has the capability of receiving a selectively encrypted/scrambled transport stream such as produced by the equipment in Fig. 1, having the encrypted/scrambled transport stream converted into a clear stream by means of the module 30, and forwarding a video/audio to signal an appliance such as a TV set.

With reference to Fig. 12, a selectively encrypted transport stream SETS is received, and encrypted data packets are extracted for decryption or descrambling by circuitry on SC 40. The user key for such decryption is stored in a safe memory of SC 40. This step is referred to as "Packet descrambling" in Fig. 12. Asa next step, the descrambled data packets are inserted in the buffered transport stream at locations corresponding in time to the original positions in the base transport stream BTS. As a result, a clear transport stream CTS is obtained.

In this embodiment, the selective decryption is performed with circuitry on the SC 40. This is possible because the selective encryption proposed here can be dealt with on the user side with a moderate hardware performance requirement, as is typically embodied in a smart card. In other embodiments of the invention,

however, the selective decryption may be performed by circuitry incorporated in, or software/firmware residing in, module 30.

With reference to Figs. 2 to 6, different embodiments of the head-end component are shown but they all may have the same functionality as that in Fig. 1. Specifically, the Fig. 1 embodiment works without a PC, and the encryption of the selected data packets is performed in module 26 which is a PC card smart card reader for SC 14. Alternatively, the encryption may be performed by circuitry on SC 14, as shown in Fig. 3 where the SC 14 has a scrambler 29 . The selection of the data packets to be encrypted is either performed by software executed by a microprocessor 27 within module 26 or by a hardware filter incorporated in module 26. In Fig. 4, the scrambler 29 is shown as incorporated in module 26. In Fig. 5, the functionality of module 26 is incorporated in STB 18, which is equipped with a smart card reader 13 for SC 14. The scrambler 29 is incorporated in SC 14. In Fig. 6, the only difference over Fig. 5 is that the scrambler 29 is incorporated in STB 18.

With reference to Figs. 8, details of the user smart card (SC) 40 (see Fig. 7) are shown. SC 40 has an interface 35 that corresponds to interface 34 in module 30. It also has a private packet descrambler 50 for the decryption of the selectively encrypted data packets, and a microcomputer 52 with a microprocessor and a memory for storing an event key, or a user key in case of an event key to be down-loaded with the EMMUs. In Fig. 8. it is assumed that SC 40 is a "Pay Per Event Smart Card".

With reference to Figs. 9 and 10, different embodiments of the user component are shown but they all may have the same functionality as that in Fig. 7. Specifically, in the Fig. 9 embodiment, the user component includes a user Set-Top-Box (STB) 37 with an interface 39 for module 30. Module 30 has incorporated therein a conventional DVB descrambler 41. In this embodiment, decryption of the selected data packets is performed on SC 40 while DVB descrambling is performed on module 30 which is a conditional access module (CAM) upgraded to cope with the needs of selective data packet encryption. In the

Fig. 10 embodiment, the functionality of module 30 has been incorporated in STB 37, as is known from conventional embedded conditional access systems. Accordingly, STB 37 has an interface 53 for SC 40. Decryption of the selectively encrypted data packets is still performed by circuitry on SC 40, i.e. by descrambler 50.

Having disclosed basic embodiments of the invention, further improvements are apparent from Figs. 13 and 14.

In Fig. 13, the processing of a data packet for selective encryption is shown in detail. The data packets selected here for encryption are preferentially those the contents of which are propagated to succeeding data packets in an MPEG transport stream so that a relatively powerful scrambling effect is achieved wit a relatively reduced percentage of encrypted data packets. This is an important factor if the decryption of the selectively encrypted data packets is to be performed on a smart card with inherently moderate processing capacity, but with an inherently high level of security.

In Fig. 14, the generation of a partially DVB-scrambled and selectively encrypted transport stream is illustrated. As is easily seen, all data packets other than the selectively encrypted data packets are DVB-scrambled. Specifically, a clear content is partially selectively encrypted and partially DVB scrambled, the DVB keys being processed from the clear content of selectively encrypted packet.

By this way, a stream completely scrambled without using EMM to broadcast DVB keys is provided. The scrambled stream contains the CW that are processed from a selectively encrypted packet that has been decrypted. The level of security is still high as those control words could only be recovered if the "one-event card" is available to decrypt the selectively encrypted packets. This solution has the advantage that the stream is completely scrambled and that the content's broadcast is independent from EMMs so independent from broadcasting companies (as TPS, Canal + ...etc).

In figure 14, the process to have the scrambling stream is illustrated:

- to-be-selectively-encrypted packets are sel 1, sel 2, sel 3
- To-be-DVB-scrambled packets are 1.1,1.2, ...,1.n,2.1,2.2,...,2.n,3.1, 3.2...
- CW(Sel i) is the control word calculated from clear Sel i content and that will be used to scramble packets i.1,i.2,....,i.n
- As soon as CW (Sel i) is processed, Sel i is encrypted in the head end Smart Card (for example)
- CW(Sel i) is fed to the DVB scrambler to processed the scrambled i.1,i.2,....,i.n
- Encrypted Sel i is inserted in advance to i.1,i.2,.....,i.n

When a user STB receives the scrambled stream,

- it will send encrypted packet Sel i to the smart card,
- The smart card will decrypt Sel i,
- The smart card will process CW(Sel i),
- Sel i will be sent to the DVB descrambler,
- The DVB descrambler will descramble packets i.1,i.2,....,i.n with Sel i.

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.